

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

United States of America
v.

VALERICA IVANOVICI
a/k/a Jeno Urban
a/k/a Zoltan Toth
a/k/a Velerica Eugen

Defendant(s)

Case No. 1:20-mj-00098

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of August 7, 2019-September 29, 2019 in the county of Hamilton in the
Southern District of Ohio, the defendant(s) violated:

Code Section

Offense Description

18 U.S.C. 1029(b)(2)
18 U.S.C. 1349

Conspiracy to Commit Access Device Fraud
Conspiracy to Commit Bank Fraud

This criminal complaint is based on these facts:

See Affidavit

☒ Continued on the attached sheet.

Devin Peugh

Complainant's signature

Devin Peugh, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: Feb 5, 2020

Stephanie K. Bowman

Judge's signature



City and state: Cincinnati, Ohio

Hon. Stephanie K. Bowman, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT

I, Devin Peugh, being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent of the Federal Bureau of Investigation since March 2019, and am currently assigned to the Cincinnati Division. Prior to my employment as a Special Agent, I was employed for five years as a Staff Operations Specialist for the Federal Bureau of Investigation, assigned to the San Diego Division. While employed by the Federal Bureau of Investigation, I have investigated federal criminal violations related to high technology or cybercrime, child pornography, terrorism, money laundering, and credit card fraud. I have gained experience through training at the Federal Bureau of Investigation and everyday work relating to conducting these types of investigations. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

2. I make this Affidavit in support of an application for a criminal complaint and arrest warrant for **VALERICA IVANOVICI (IVANOVICI)** (also known as Jenő Urban, Zoltan Toth, and Valerica Eugen); **GEORGIAN GOREA (GOREA)** (also known as József Harsányi); and others, for a violation of 18 U.S.C. § 1029(b)(2) (conspiracy to commit access device fraud) and 18 U.S.C. § 1349 (conspiracy to commit bank fraud). The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other law enforcement officers and witnesses. This Affidavit is intended to show there is sufficient probable cause for the charges in the complaint and does not set forth all of my knowledge about this matter.

BACKGROUND ON CREDIT CARD SKIMMERS

3. The FBI has been investigating a credit card fraud scheme which utilizes skimming devices (“skimmers”) placed on and inside ATMs in the Southern District of Ohio, which acquire credit and debit card information from victims.

4. Based on my training and experience, I know that it is possible to re-encode digitally stored account information onto the magnetic strip of any type of plastic access device using commercially available digital reader-writer devices and the corresponding computer software that comes with the devices. These devices and this software have legitimate commercial uses such as coding hotel room keys and creating security badges.

5. Based on my training and experience, I know that subjects that use fraudulently re-encoded credit and debit cards purchase prepaid credit cards as a way to conceal the illegitimate source of funds and carry on the fraud. Prepaid credit and debit cards are also a common tool for perpetrators of fraud and identity theft. The perpetrators can also use the prepaid cards to re-encode compromised credit card account data onto access devices which they then use to make fraudulent purchases such as additional prepaid credit cards at stores such as Walmart and Kroger.

6. The process of purchasing prepaid credit cards at retail stores involves the transmission of electronic communications via wire communication between the point of sale and the bank that holds the compromised account that is being charged for the transaction, and the bank that issued the prepaid credit card. These communications are transmitted in interstate commerce because the various banks are located in different states from each other and from the points of sale, and because communications sent via wire communications travel interstate based on the locations of the service providers.

7. Through my training and experience, I know skimmers to be devices used to covertly collect credit and/or debit card data from victims. The illegally collected credit and debit card numbers are considered access devices. The credit and debit card number related to a victim's account and the cards and card numbers are issued by banks which are federally insured financial institutions.

8. A “skimmer” placed inside an ATM collects card information from victims when that victim uses a card at the ATM. The skimmer is installed between the credit card reader and the other internal circuitry of the ATM. In addition to the skimmer, the subjects may also install a camera on the face of the ATM to capture entries made by customers on the pin pad of the ATM. This is used to obtain both the card number and corresponding PIN for the card.

9. The skimmer usually does not keep the ATM from otherwise functioning properly; the intended transaction will typically proceed without interruption of any kind or any notification to the victim or third party. Because of this and the fact that the skimmer is installed inside the ATM, it is impossible for victims using the ATM to detect the presence of the skimmer. Additionally, the skimmer does not require a successful transaction to collect the card data; the card data is collected when the victim swipes their card.

10. A single skimmer is capable of storing card information for hundreds of victims. A credit or debit card contains a magnetic strip that contains information such as the card holder's name, card number, and expiration date. The victim card data is then used to create a clone of the compromised credit card by re-encoding another card, such as a prepaid card or gift card, with victim card information.

11. To make the card appear more legitimate to third parties, the subjects may use a credit card embossing device to physically stamp a name of their choosing onto the newly written card.

12. Based on my training and experience, I know that individuals involved in ATM skimming activity typically use re-encoded cards at ATMs to withdraw cash from the associated account. The subjects use a variety of equipment to re-encode cards such as card reader/writers, laptops or computers with software specifically designed to read/write data to cards.

13. Based on my training and experience, I know that individuals sometimes work in groups in furtherance of skimming activity. Once an individual manufactures a skimmer, that individual will use the skimmer in one or more of the following ways: First, the individual can personally use the skimmer to collect card information. Second, the individual can sell the device to another person who will then use the device to collect card information. Third, the individual can provide the device to another person in return for a portion of cards collected by the device as payment. The re-encoded cards can then be used to purchase prepaid goods and services, cashed out, or sold to other individuals.

14. Based on my training and experience, I know that individuals involved in skimming sometimes travel from one region to another inserting skimmers, re-encoding cards, and conducting cash out ATM transactions. This sometimes requires individuals involved in skimming to travel with the requisite electronics to conduct skimming activities.

PROBABLE CAUSE

15. Financial Institution-1 located in Colerain Township, Ohio, and headquartered in the Southern District of Ohio, detected a skimmer at one of its ATMs (hereafter ATM-1). Camera footage from ATM-1 revealed the following:

- a. On August 7, 2019, an individual (hereafter Individual-1) approached ATM-1 on foot. Individual-1 removed a dark bar from his sweatshirt and placed it below the face of ATM-1. Based on my training and experience, I know that when installing a skimming device individuals will typically also install a camera facing the pin pad of the ATM in order to capture the PIN numbers entered by customers. Individual-1 departed from ATM-1 on foot.
 - b. On August 7, 2019, approximately six minutes later, an individual identified as defendant **GEORGIAN GOREA (GOREA)**, approached ATM-1 on foot carrying what appeared to be an electronic device. **GOREA** inserted the device into ATM-1's card reader. **GOREA** removed a card from his wallet and inserted the card into ATM-1's card reader. **GOREA** inserted the card into ATM-1's card reader multiple times while manipulating the face of ATM-1. **GOREA** did not receive any cash or receipts from ATM-1. Based on my training and experience, I believe **GOREA** installed a skimmer inside of ATM-1 and inserted cards to ensure it had been installed properly. **GOREA** departed from ATM-1 on foot.
16. On August 11, 2019, at approximately 8:58pm, Individual-1 approached ATM-1 on a bicycle. Individual-1 removed a contraption from the basket of the bicycle. Individual-1 used this contraption to remove a device from ATM-1. Individual-1 removed the black bar installed beneath the face of ATM-1, then departed.
17. Approximately 342 debit card numbers were compromised as a result of the skimming device installed on ATM-1 from August 7, 2019, to August 11, 2019.
18. Camera footage showed the installation and removal of another skimming device at a Financial Institution-1 ATM located in Celina, Ohio between September 28 and 29, 2019. A

review of this footage revealed the following information:

- a. On September 28, 2019, at approximately 7:15am, defendant **GOREA** arrived at the ATM in a dark color Toyota sport utility vehicle. **GOREA** then exited the vehicle and, after multiple attempts, successfully installed an electronic device into ATM's card reader. **GOREA** then inserted a magnetic stripe card into ATM's card reader. **GOREA** returned to the vehicle and maneuvered the vehicle closer to ATM. After re-positioning the vehicle, ATM's camera captured **GOREA** manipulating and compromising the face of ATM. **GOREA** then installed a black bar beneath the face of ATM.
- b. On September 29, 2019, at approximately 8:56am, **GOREA** approached the ATM in a dark color Toyota sport utility vehicle. **GOREA** proceeded to remove a black bar from beneath the face of ATM and departed.

19. Video and photos also show that defendants **GOREA, IVANOVICI**, and others used the compromised card numbers taken from Financial Institution-1 to conduct cash withdrawals at approximately 16 ATMs operated by Financial Institution-2 between August 31, 2019 and September 3, 2019. These 16 ATMs were located in the Southern District of Ohio, with the majority located in the Cincinnati metropolitan area.

20. Visa application pictures for **GOREA** appear to show the individual captured in the ATM photos previously discussed. **IVANOVICI**'s identity was determined through a comparison of ATM photos with a photograph used by **IVANOVICI** on a prior visa application.

21. On July 1, 2019, local and federal law enforcement agencies conducted a search of a vacation rental in Louisville, Kentucky rented by **IVANOVICI** using the alias "Zoltan Toth" after owner of the residence reported that **IVANOVICI** had left what the owner believed

to be suspicious materials in the residence. The owner discovered these materials following **IVANOVICI's** departure from the rental and consented to law enforcement conducting a search of the rental. This search identified materials that law enforcement officers believed were used to build skimming devices in **IVANOVICI's** rented residence.

CONCLUSION

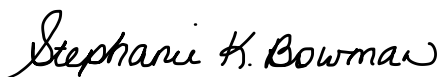
22. Based on the information above, I respectfully submit that there is probable cause to believe that **GEORGIAN GOREA, VALERICA IVANOVICI**, and others conspired to violate 18 U.S.C. § 1029(b)(2) and 18 U.S.C. § 1349 from on or about August 31, 2019 through at least September 29, 2019. I respectfully request that the Court authorize the complaint and issue an arrest warrant.

Respectfully submitted,



Devin Peugh
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on February 5, 2020



HONORABLE STEPHANIE K. BOWMAN
UNITED STATES MAGISTRATE JUDGE

